Glisland® Training Series:

21 CFR Part 11 Requirements & *Implementation*

Glisland, Inc.
San Jose, California, USA
http://www.glisland.com

About the Speaker

Luke G. Liang, PhD, RAC

Luke's knowledge and experience in 21 CFR Part 11 compliance came from unique combination of all three perspectives: regulatory affairs (he was Director of QA and Regulatory Affairs at iMetrikus), customers (he was Principal Scientist and Manager at Johnson & Johnson), and software vendors (he was Software Architect at WebMD in charge of 21 CFR Part 11 compliance for Clinical Trial software development and Principal Engineer and Manager at Caliper Life Sciences designing and developing Lab-on-a-Chip software applications with features for compliance support). He holds RAC (Regulatory Affairs Certified).

Objectives

1. Analyze the regulatory provisions section by section to understand each requirement.
2. Explain what it takes to comply with each of the regulatory requirements from users' perspective.
3. Provide solutions for designing a software system that can meet user requirements for regulatory compliance.

A Brief History of 21 CFR Part 11

- **July 1992:** The first draft published
- **March 1997:** Final rule published
- **August 1997**: Part 11 became effective
- **July 1999:** Enforcement policy released
- **2001-2002:** Various draft guidances published
- **February 2003:** Enforcement policy and draft guidances withdrawn
- **February 2003:** New draft guidance issued: narrow interpretation
- **August 2003:** Final guidance (Scope and Application Guidance) published
- **May 2007:** *Guidance for Computerized Systems Used in Clinical Investigations* supplements the August 2003 guidance
- **Current Status:** Re-examination period

FDA Final Guidance (Aug. 2003)

"Part 11 will be interpreted narrowly; we are now clarifying that fewer records will be considered subject to part 11.

For those records that remain subject to part 11, we intend to exercise enforcement discretion with regard to part 11 requirements for validation, audit trails, record retention, and record copying in the manner described in this guidance and with regard to all part 11 requirements for systems that were operational before the effective date of part 11 (also known as legacy systems).

We will enforce all predicate rule requirements, including predicate rule record and recordkeeping requirements."

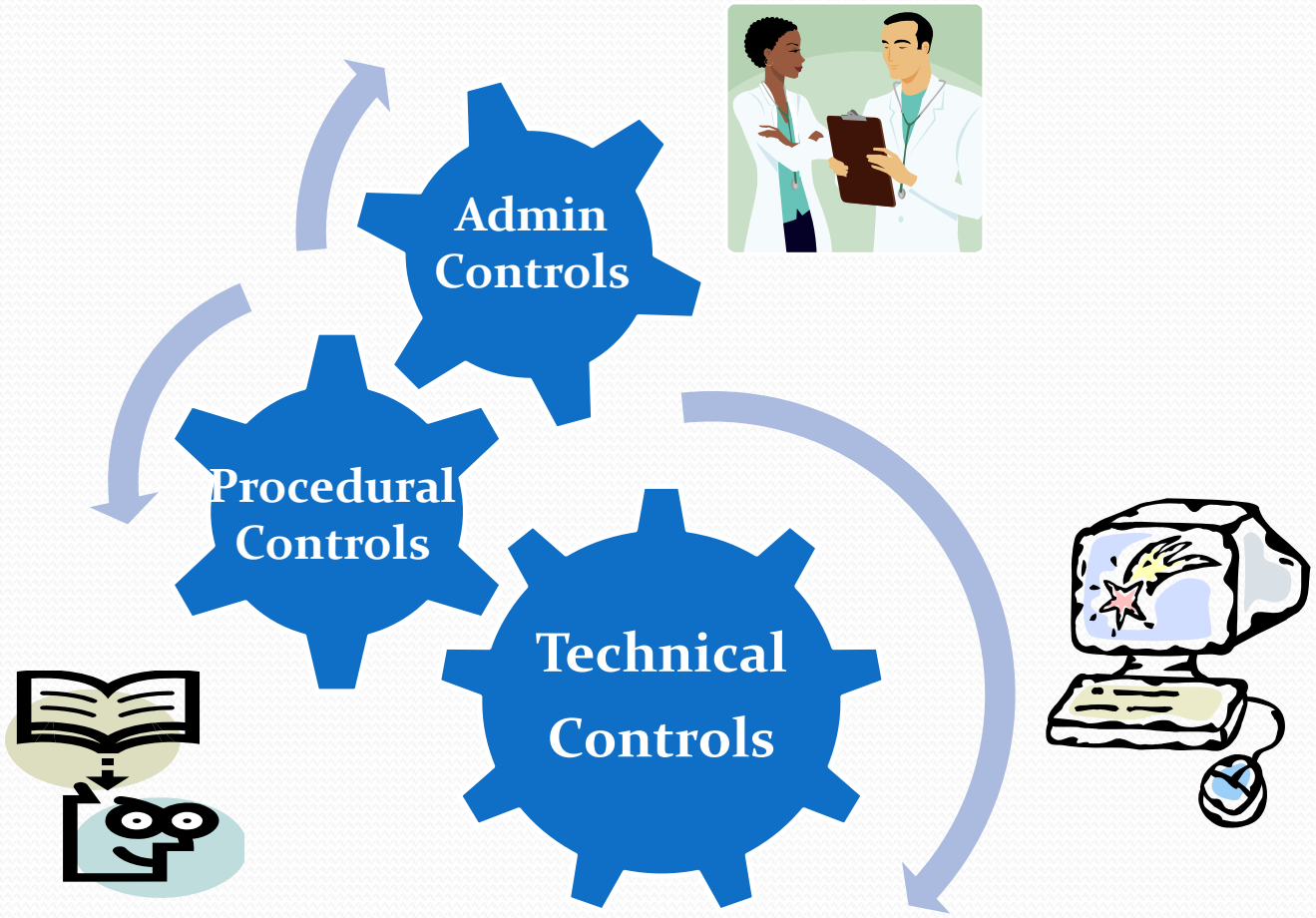
Enforced rules and requirements

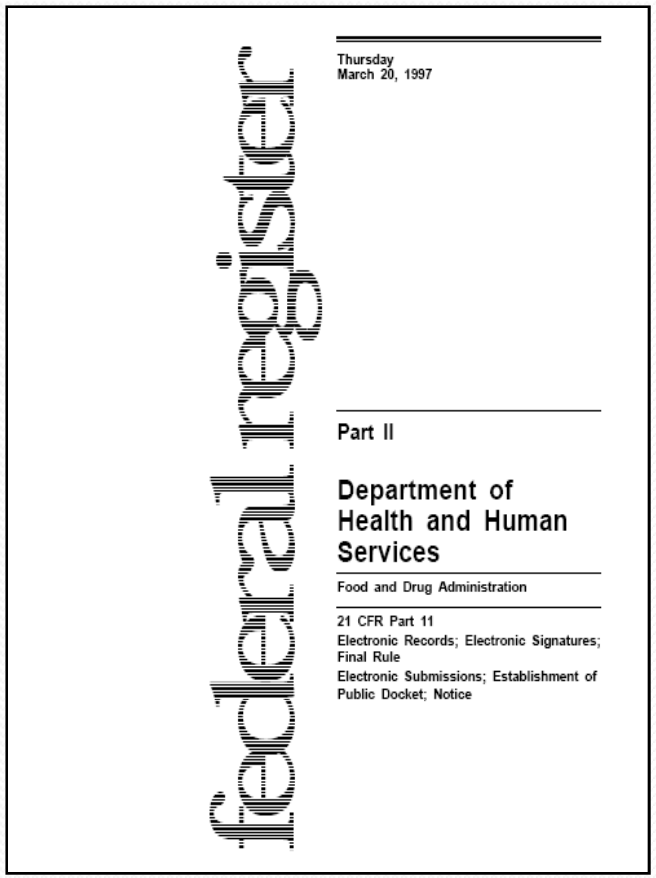
1. limiting system access to authorized individuals
2. use of operational system checks
3. use of authority checks
4. use of device checks
5. determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
6. establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
7. appropriate controls over systems documentation
8. controls for open systems corresponding to controls for closed systems bulleted above (§ 11.30)
9. requirement related to electronic signatures (e.g., §§ 11.50, 11.70, 11.100, 11.200, and 11.300)

21 CFR Part 11
Electronic Records; Electronic Signatures

Subpart A General Provisions
Subpart B Electronic Records
Subpart C Electronic Signatures

Controls for Compliance





Subpart A
General Provisions

11.1 Scope
11.2 Implementation
11.3 Definitions

§ 11.1 Scope (a)

The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

- Electronic vs. paper form
  - Electronic records
  - Electronic signatures
  - Handwritten signatures executed to electronic records
  - Trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

§ 11.1 Scope (b)

This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

- Part 11 records:
  1. Records in electronic form
  2. Required to be maintained under predicate rules
  3. Submitted for regulatory filing
  4. Operations: create, modify, maintain, archive, retrieve, transmit

- Not Part 11 records:
  1. Paper records
  2. Paper records transmitted by electronic means
     (e.g. fax or email attachments of copy of paper records)

§ 11.1 Scope (c)

Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

- Controls to ensure Part 11 requirements are met:
  - Administrative Controls
    - Set policies, assign responsibilities, training, notification, auditing…
  - Procedural Controls
    - SOPs, validation, calibration, IQ/OQ/PQ…
  - Technical Controls
    - Computerized features to assist/enforce administrative/procedural controls
- 21 *CFR* 11 effective date: August 20, 1997

§ 11.1 Scope (d)

Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

- Users should decide on whether to electronic records or paper records.
- The use of electronic records for regulated activities is subject to 21 CFR Part 11 rules.

§ 11.1 Scope (e)

Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

- What should be available for FDA inspection?
  1. Computer systems (hardware and software)
  2. System validation records
  3. IQ/OQ/PQ/Calibration
  4. SOPs
  5. Logbooks, audit trails

§ 11.1 Scope (f)

This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

- *21 CFR Part 1* sets forth regulations for food industry.
- *21 CFR 1.326 – 1.368* and *21 CFR Part 1 subpart* J are the same thing. Those records are not subject to Part 11.
- The second sentence refers to records specified in Section 1.329 titled: "Sec. 1.329 Do other statutory provisions and regulations apply?" which are subject to Part 11.

§ 11.2 Implementation (a)

For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

- Records required to be maintained by predicate rules
  - GLP, GCP, GMP, QSR…
- Options to use paper or electronic form in whole or in part to meet predicate rule requirements
  - Flexibility in system requirement/design to provide the technical controls for compliance support
  - Set compliance boundary for electronic records in the system
  - Hybrid systems



§ 11.2 Implementation (b)

For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

- Option of submitting records to FDA in paper or electronic form, in whole or in part
- If the users choose to submit the records to FDA in electronic form, 21 CFR Part 11 must be met
- Hybrid systems
- Encryption, check sum, review support

§ 11.2 Implementation (b)

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Check Docket No. 92S-0251 on FDA website for file formats

Docket No. 92S-0251

U.S. Food and Drug Administration

U.S. Department of Health and Human Services

FDA Home Page | Dockets Home Page | Dockets Contacts and Location | Operating Status | Item Code Definitions

Up

92S-0251: Electronic Submissions
Federal Register Date: 03/20/97
Page No.: 13467

- Center for Biologics Evaluation and Research
- Center for Drug Evaluation and Research
- Center for Food Safety and Applied Nutrition
- Center for Veterinary Medicine
- Office of Regulatory Affairs
- Office of Orphan Products Development

Center for Biologics Evaluation and Research

Notice: 2

Received: 8/7/06
Published in the Federal Register: 8/8/06 71FR45057
Submitter: CBER
Record Name(s): Electronic Gateway [HTM] [PDF]
Effective Date: August 8, 2006

§11.3 Definitions

- Electronic Record
- Electronic signature
- Digital Signature (an electronic signature based on cryptographic method)
- Biometrics
- Closed System
- Open System

Subpart B
Electronic Records

- 11.10 Control for closed systems
- 11.30 Controls for open systems
- 11.50 Signature manifestations
- 11.70 Signature/record linking

§11.10 Controls for closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

- Ensure the authenticity, integrity, confidentiality of electronic records:
  - records generated from reliable source/raw data for authenticity
  - employ checksum/hash to check integrity
  - employ audit trails to track record history

- Prevention of signature repudiation:
  - check signing authority
  - employ audit trails
  - link signature to records signed
  - employ rules for undoing signature

§11.10 Controls for closed systems (a)

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

- Validation objectives
  - Accuracy
  - Reliability
  - Consistent intended performance
  - Ability to discern invalid or altered records (e.g. applying checksum)
- Design/validation strategy
  - Risk-based approach

§11.10 Controls for closed systems (b)

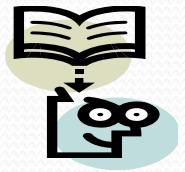
The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

- Copies of Records:
  - Must be accurate and complete
  - In both human readable and electronic form
  - Suitable for inspection, review and copying by FDA (examples of such formats include, but are not limited to, PDF, XML, or SGML)

§11.10 Controls for closed systems (c)

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

- Procedural Control:
  - Specify record retention requirements
  - Establish record retention procedures



- Technical Controls:
  - Off-line or network backup or archive of records to meet retention time requirements specified in the SOPs
  - Readily retrieve backup or archived records
  - Validate data accuracy in retrieving process
  - Backward compatibility

§11.10 Controls for closed systems (d)
Limiting system access to authorized individuals.

- Administrative Controls
  - Limit access to the building
  - Limit access to the hardware devices
  - Limit access to the computer system

§11.10 Controls for closed systems (e)

Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

- Technical Controls
  - Built-in independent audit trail module:
    1. *Use separate database tables or file to store audit trail data*
    2. *Record User ID, name, date time, action (create, modify, delete)*
  - Append change history in current version
  - Use versioning allowing to retrieve previously recorded information
  - Show/print audit trail reports for review and copying

§11.10 Controls for closed systems (f)

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

- Technical Controls
  - Document permitted sequencing of steps and events.
  - Ensure that the system has functionality to enforce the steps and events follow the documented sequence.
  - Validate the system to ensure the system does as what is supposed to do.
  - Example: running daily calibration, collecting background data, checking signal to noise ratio… before running sample.

§11.10 Controls for closed systems (g)

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

- Procedural Controls
  - Define role and responsibilities
- Technical Controls:
  - User account management
  - Role based access

§11.10 Controls for closed systems (h)

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

- Technical Control:
  - The predicate rules require computerized system be validated. The validated device IDs (i.e. instrument serial number) is kept in the security system.
  - The system checks the validity of devices before data acquisition.
  - Advanced features:
    - Associate device ID with IQ/OQ/PQ status.
    - Record device logs with IQ/OQ/PQ status.
    - If the device is replaced or serviced, IQ/OQ/PQ are required.
    - Ability to updated device ID (e.g. replace existing device with new one or adding new device).

§11.10 Controls for closed systems (i)

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

- Administrative control:
  - Conduct and manage the required trainings
  - Include developers, administrators, and users of the systems
- Procedure Control:
  - SOP specifies education, training, and experience requirements
- Technical Control:
  - Allows system administrator to enter training results for users and checks/reports records of training requirement (e.g. expiration date)



§11.10 Controls for closed systems (j)

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

- Procedural Controls:
  - Establish SOPs (e.g. signature password policy).
  - Define roles and responsibilities.

- Administrative Control:
  - Conduct training.

- Technical Control:
  - Role based functional access.
  - Policy reminder before executing a signature

    (e.g. "I understand that electronic signatures are legally binding equivalent of my handwritten signature.")

§11.10 Controls for closed systems (k)

Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

- Administrative controls
  - Control system documents (user guide, SOPs, IQ/OQ/PQ/Calibration criteria, operation log)
  - Ensure that the right version of documents are used for conducting training and operation.

- Technical controls
  - Client software provides online read-only user guide.
  - The system tracks the history of systems documentation in audit trail.
  - IQ checks the proper version of user guide is installed.

§ 11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

- Example of open systems to consider:
  - Transmit data through internet (e.g. eSubmission or data from CRO)
  - Store data copy in potable devices (e.g. CD or USB drive)
- Additional controls required:
  - Data encryption
  - Digital signature

§ 11.50 Signature manifestations (a)

Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

- Technical Controls:

  Ensure that following information is contained in the signed electronic records:

  (1) The printed name of the signer;

  (2) The date and time when the signature was executed; and

  (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

§ 11.50 Signature manifestations (b)

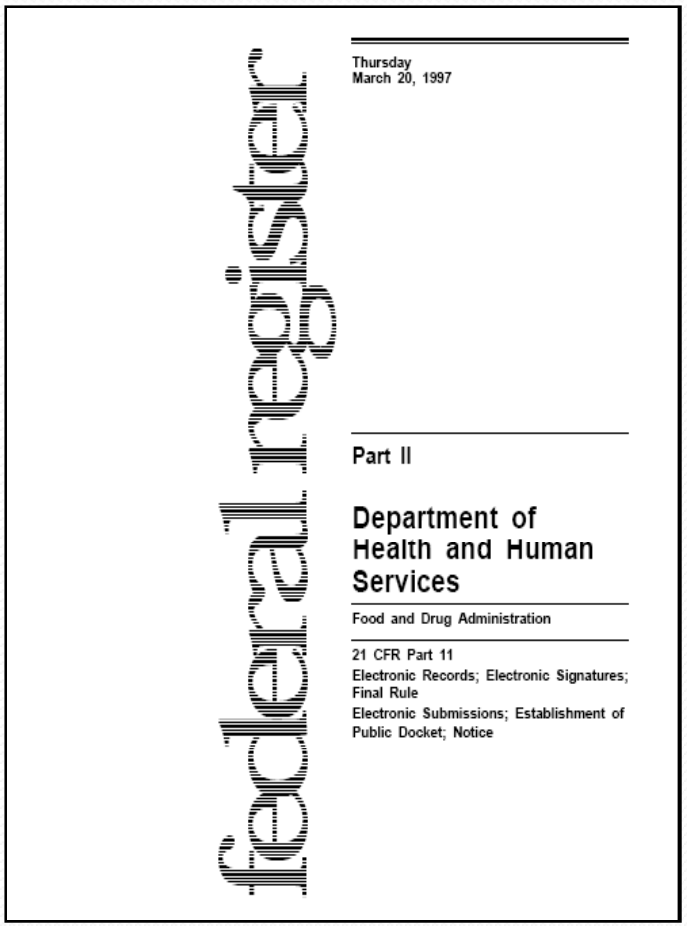
The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

- Electronic signatures are electronic records.
- Technical control:
  - The information of electronic signature is associated to, or stored in, the same file, and subject to the same security controls as the records undersigned
  - The electronic signature is also kept in the audit trail as part of operation records (who do what and when)
  - The signature is available for display or printout as integral part of signed records

§ 11.50 Signature/record linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

- Technical controls:
  - Closed systems:
    - User ID & Password access control.
    - Role based signature authorization.
    - Use pen pad device to capture handwritten signature.
    - Embed signature in the record undersigned.
    - Record hash codes before and after signature.
  - Additional controls for open systems:
    - Sign records with private key.
    - Encrypt records and signatures with private key.



Subpart C
Electronic Signatures

11.100 General requirements

11.200 Electronic signature components and controls

11. 300 Controls for identification codes/passwords

§ 11.100 General requirements (a)

Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

- Technical controls:
  1. The electronic signature is based on the unique combination of user ID and password
  2. The system ensures that a user ID is unique and once it is created, it cannot be reused by, or reassigned to anyone else
  3. If PKI is used, ensure that each certificate is unique

Unique

§ 11.100 General requirements (b)

Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

- Administrative controls:
  1. Document individual's identity (e.g. employment record)
  2. Verify the individual identity at the time of account creation

- Procedural control:

  Establish policy to verify the identity when creating signature account

- Technical control:

  Option to use network account that has the user identity documented at the time of employment or signing contract

ID check

§ 11.100 General requirements (c)

Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

"Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures."

Certify

§ 11.200 Electronic signature components and controls(a)

Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password. (i)When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.)(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

- Technical Controls
  1. Ensure that a user ID is unique and correct password is provided for signature
  2. The system remember who does signing last time to avoid entering the same user ID every time in the case of executing a series of signings during a single continuous session

E-sign

§ 11.200 Electronic signature components and controls (a)

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

- Administrative control:
  - Establish no-password-sharing policy and train each user

- Procedural control:
  - Define authority of signature delegate and witness

- Technical control:
  - Provide delegate signing power to sign on behalf of others with witness
  - Include delegate and witness ID in the signature and mark something like “signed on behalf of …, witnessed by…”

Genuine owner

§ 11.200 Electronic signature components and controls (b)

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

- Example: fingerprint device.
- Validation
  1. Unique and measurable
  2. Cannot be used by other than genuine owner

Genuine owner

§ 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

- Technical controls:
  1. The software ensures that no two users have the same user ID. It is possible that users may have the same password but it shouldn't check so to give the hint that there is a valid password for some one else.
  2. Once a user ID is issued, it can be disabled but cannot be deleted from the system to ensure that it will not be assigned to different person.

Unique ID

§ 11.300 Controls for identification codes/passwords.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

- Technical controls:
  1. Allows system administrator to set password expiration policy.
  2. The software enforces the password expiration policy by reminding password expiration date and requiring users to change password upon the expiration date.
  3. The event of password change is kept in audit trail.

ID / Pswd check

§ 11.300 Controls for identification codes/passwords.

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

- Technical controls:
  1. The software allow the system administrator to permanently disable a login devices with notes and to create a new one.
  2. A permanently disabled login device is marked as so in the database to prevent it from be reactivated by mistake.

Loss control

§ 11.300 Controls for identification codes/passwords.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

- Technical controls:
  1. The software allows the administrator to set maximum number of failed login according to the company's policy
  2. The software automatically locks the user ID exceeding the maximum number of failed login and email the user to contact the administrator
  3. Only the administrator can unlock the user ID
  4. Record failed logon events in the audit trail and notify appropriate organization unit via email

Transaction safeguard

§ 11.300 Controls for identification codes/passwords.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

- Technical controls:
  - Valid protocols to check the integrity of security access devices
  - Validate security access devices before granting the access

Device check

References

1. *21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule,* Federal Register, March 20, 1997
2. *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures — Scope and Application,* FDA, August 2003
3. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*, FDA, 2002
4. *Guidance for Industry, Computerized Systems Used in Clinical Investigations*, FDA, May 2007

Glisland Services for 21 CFR Part 11 Compliance

- provide training on 21 CFR Part 11 requirements and implementation
- assess current state and indentify gaps
- analyze the risks
- design and develop software systems for compliance technical controls
- validate software systems per 21 CFR Part 11 requirements
- develop SOPs (Standard Operation Procedures) for 21 CFR Part 11 compliance practice
- prepare 21 CFR Part 11 implementation document ready for marketing use